

1 LAURENCE F. PULGRAM (CSB No. 115163)
lpulgram@fenwick.com

2 LIWEN A. MAH (CSB No. 239033)
lmah@fenwick.com

3 FENWICK & WEST LLP
555 California Street, 12th Floor
4 San Francisco, CA 94104
Telephone: (415) 875-2300
5 Facsimile: (415) 281-1350

6 PATRICK E. PREMO (CSB No. 184915)
ppremo@fenwick.com

7 HENRY Z. CARBAJAL III (CSB No. 237951)
hcarbajal@fenwick.com

8 DENNIS M. FAIGAL (CSB No. 252829)
dfaigal@fenwick.com

9 FENWICK & WEST LLP
Silicon Valley Center
10 801 California Street
Mountain View, CA 94041
11 Telephone: (650) 988-8500
Facsimile: (650) 938-5200

12 Attorneys for Plaintiff
13 SUCCESSFACTORS, INC.

14 UNITED STATES DISTRICT COURT
15 NORTHERN DISTRICT OF CALIFORNIA
16 OAKLAND DIVISION

17
18 SUCCESSFACTORS, INC. a Delaware
corporation,

19 Plaintiff,

20 v.

21 SOFTSCAPE, INC., a Delaware
22 corporation; and DOES 1-10,

23 Defendants.

Case No. C-08-1376 CW (BZ)

**DECLARATION OF KEVIN MOORE IN SUPPORT
OF PLAINTIFF SUCCESSFACTORS, INC.'S
REPLY MEMORANDUM IN SUPPORT OF ITS
MOTION TO COMPEL PRODUCTION OF
DOCUMENTS, FURTHER INTERROGATORY
ANSWERS AND PROPER PRIVILEGE LOGS**

Date: September 3, 2008
Time: 10:00 a.m.
Judge: Hon. Bernard Zimmerman
Place: Courtroom G, 15th Floor

Date of Filing: July 30, 2008
Trial Date: May 11, 2009

1 I, Kevin Moore, declare as follows:

2 1. I am the Director of the Information Technology department, and senior forensic
3 investigator, at the law firm of Fenwick & West LLP ("Fenwick"), counsel to Plaintiff
4 SuccessFactors, Inc. ("SuccessFactors"). I make this declaration in support of Plaintiff
5 SuccessFactors, Inc.'s Reply Memorandum in Support of its Motion to Compel Production of
6 Documents, Further Interrogatory Answers and Proper Privilege Logs. I make the following
7 statements based upon my personal knowledge, and, if called upon to testify, would testify
8 competently to them.

9 2. I have a Bachelor of Science degree from San Francisco State University and 45
10 units of graduate division courses in Information Services from the University of Phoenix. I have
11 more than 23 years of experience in the computer industry from software development to system
12 design and engineering.

13 3. In my current position as senior forensic investigator, I specialize in conducting
14 and managing our litigation support processes. This work includes on-site and remote data
15 collection including forensic data collection and analysis. I have worked in the field of legal
16 information technology for ten years and have worked in the field of forensic analysis of
17 computer and electronic data for eight years. In that capacity, I have lead the forensic
18 investigations for Fenwick in dozens of matters.

19 4. I began my formal training in computer forensic analysis and investigations eight
20 years ago at NTI, the leading provider of forensic software and certification courses. I have kept
21 my computer forensic training current with additional courses from Guidance Software, Access
22 Data and NTI, and currently hold the EnCe certification for use of EnCase software from
23 Guidance Software.

24 5. I have been a principal presenter on the topic of forensic analysis, e-discovery,
25 compliance and information security at many conferences, client meetings and internal training
26 sessions. I was a principal presenter on these topics at the annual California State Bar conferences
27 in 2006 and 2007 and at the International Legal Technology Association Annual Conference in
28 2006.

1 6. I understand that Defendant Softscape, Inc. represents that it has no separate
2 document management system or program, such as Hummingbird DM, residing on its server
3 system or network.

4 7. Even assuming this were the case, some log file and metadata information for
5 collected documents nevertheless would exist on Softscape's server as well as within the forensic
6 images made of its computers and hard drives by virtue of the presence of the Microsoft
7 Windows environment and the use of e-discovery tools such as EnCase for the search, extraction
8 and collection of electronically stored information.

9 8. This residual log and metadata information can be ascertained without much
10 difficulty given that search, collection and production of documents by Softscape has already
11 taken place. Proper use of e-discovery tools such as EnCase, would dictate that this information
12 would have already been tagged in conjunction with the search for documents, which could then
13 be used to quickly create a report based on "bookmark" or "search term" hits pointing to the
14 original file and disclosing its file path and file system metadata. For example, use of EnCase or
15 other similar e-discovery tools to search for, extract and collect of documents, when performed
16 properly will produce "chain of custody" or file path information, which can also be referred to as
17 an audit log file or "bookmark," showing where collected documents were found and where they
18 are located within the searched computer systems and the overall file directory structure of the
19 searched systems, as well as an MD5 Hash, which is a digital fingerprint for each extracted file.

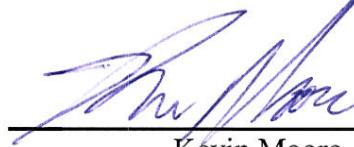
20 9. As these files were extracted using the EnCase e-discovery tool as Softscape
21 collected documents, production of the "chain of custody" or file path information should not
22 require any additional man-hours to complete.

23 10. I understand that in addition to creating a forensic image of its server, Softscape
24 also created a forensic image of individual custodians' hard drives. The file directory structure of
25 each individual hard drive is retained within the Microsoft Windows operating system running on
26 that hard drive. Thus, similar directory structure information such as that provided by audit log
27 files or "bookmarks" for individual hard drives can be extracted from those hard drives. In my
28 experience, extraction of these local drive file directory structures is not difficult as a technical

1 matter and should not require any additional man-hours to complete. Proper use of e-discovery
2 tools such as EnCase, would dictate that this information would have already been tagged or
3 "bookmarked," which in turn can be used to create a report based on "bookmark" or "search
4 term" hits pointing to the original file in the hard drive and disclosing its file path and file system
5 metadata.

6 11. Additional file system metadata is written into the Microsoft Windows operating
7 system for each individual custodian's hard drive. This file system metadata information includes
8 document creation dates, last accessed dates, last modified dates and last written dates for files
9 locally stored on the imaged hard drive. This information is similar to embedded metadata
10 included within documents produced in their native format, such as native Microsoft PowerPoint
11 files, but is not duplicative. Extraction of this local drive file system metadata is also not difficult
12 as a technical matter and should not require more than a few man-hours to complete for each hard
13 drive.

14 I declare under penalty of perjury under the laws of the State of California and the United
15 States of America that the foregoing is true and correct. Executed this 20th day of August 2008 at
16 Mountain View, California.



Kevin Moore